UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

IN THE MATTER OF THE SEARCH OF **1133 OAK HILL DRIVE, CHARLOTTESVILLE, VIRGINIA 22902, WHICH IS MORE PARTICULARLY DESCRIBED IN ATTACHMENT A**	Case No. 3:20mj00018

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Philipp W. Alhusen, being duly sworn, depose and state the following:

BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) assigned to the Richmond, Virginia (VA), Field Office, Charlottesville Resident Agency and have been so employed since 2002. As part of my duties as an FBI SA, I investigate criminal violations relating to child exploitation, in violation of 18 U.S.C. §§ 2423(a) and 2423(b), and child pornography, including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252(a), and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes, computer evidence identification, child pornography identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment, electronic items, and digital media. As a federal agent, I am authorized to

investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

2. The information contained in this Affidavit is based upon my personal knowledge and observation, my training and experience, conversations with other law enforcement officers (including officers who have engaged in numerous investigations involving child pornography and computer-based crime), and the review of documents and records.

3. I make this Affidavit in support of an application for a warrant to search the entire premises located at 1133 Oak Hill Drive, Charlottesville, Virginia (the "**SUBJECT PREMISES**"). The **SUBJECT PREMISES** is more particularly described in Attachment A, which also contains photographs of the **SUBJECT PREMISES**. The **SUBJECT PREMISES** also includes any means of storage contained in or on the yard and curtilage of the premises, including but not limited to any sheds, storage bins, trash cans, or other structures or containers regardless of size. The **SUBJECT PREMISES** also includes a grey Chrysler 300 with Virginia license plate VVZ-6888, as more fully described herein.

4. Authority is sought to search the **SUBJECT PREMISES** for the items specified in Attachment B, which constitute evidence, contraband, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252 and 2252A (possession, receipt, and distribution of child pornography) (together, the "Specified Federal Offenses"). Authority is further sought to search the entire **SUBJECT PREMISES**, including the residential dwelling and computers or computer storage media located therein, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as evidence, contraband, fruits and instrumentalities of the Specified Federal Offenses.

5. Because this Affidavit is submitted for the limited purpose of securing a search warrant for the **SUBJECT PREMISES**, I have not included each and every fact known to me concerning this

investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe the evidence of the Specified Federal Offenses is located at the **SUBJECT PREMISES**. Furthermore, the statements in this Affidavit are based, in part, on my investigation of this matter, on information provided to me by other law enforcement agents, including, but not limited to, officers who have engaged in numerous investigations involving child pornography, and the review of documents and records. Where statements of others are set forth in this Affidavit, they are set forth in substance and in part. In addition, the events described in this Affidavit occurred on or about the dates provided herein.

6. As a result of the investigation, there is probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of the Specified Federal Offenses are present at the **SUBJECT PREMISES**. Part I of this Affidavit provides relevant definitions with respect to child pornography. Part II of this Affidavit explains technical terms and concepts related to computers in general. Part III discusses common characteristics of individuals interested in child pornography and explains how computers and technology have revolutionized the way in which child pornography is produced, used, and distributed. Part IV describes the probable cause to search the **SUBJECT PREMISES**. Part V describes specific information regarding the search and seizure of computer information.

I. Definitions With Respect to Child Pornography

7. The following definitions concerning child pornography apply to this Affidavit and Attachment B to this Affidavit:

a. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

b. "Visual depictions" include, but are not limited to, undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).

c. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

d. "Minor" means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, genital-anal, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. *See* 18 U.S.C. § 2256(2).

II. Definitions and Technical Terms With Respect to Computers

8. For the purpose of this Affidavit, it also is important to understand certain technical terms and capabilities of computers and smart phones.

9. As part of my training and based on my conversations with other law enforcement agents, I have become familiar with the Internet (also commonly known as the World Wide Web), which is a global network of computers and other electronic devices that communicate with each other using various means, including standard telephone lines, high-speed telecommunications links (*e.g.*, copper and fiber optic cable), and wireless transmissions, including satellite. Due to the structure of the Internet, connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet (i) to gain access to a wide variety of information; (ii) to send information to, and receive information from, other individuals; (iii) to conduct commercial transactions; and (iv) to communicate via electronic mail ("e-mail") or through the messaging applications of various social media platforms, such as Facebook or Instagram. An individual who wants to use Internet e-mail must first obtain an account with a computer that is linked to the Internet through an "Internet Service

Provider" or "ISP" (see definition of "Internet Service Provider" below). Once the individual has accessed the Internet, whether from a residence, a university, or a place of business, that individual can use Internet mail services to send and receive e-mails, among other things. In addition, the individual can visit websites (see definition of "websites" below) and make purchases from them.

10. Set forth below are some definitions of technical terms, many of which are used throughout this Affidavit, as well as in Attachment B, pertaining to the Internet and computers more generally.

a. "Computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." 18 U.S.C. § 1030(e)(1).

b. "Computer Hardware" refers to all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes (but is not limited to) any data-processing devices (such as central processing units, and self-contained "laptop" or "notebook" computers); data storage devices (such as fixed or "hard" disks; portable or "floppy" disks; optical storage devices; flash drives, such as USB drives and memory sticks; CDs and DVDs; and electronic devices capable of storing data, such as electronic typewriters, memory calculators, personal digital assistants, and cellular telephones); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, digital cameras, and optical readers); and related communications devices (such as modems, cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

c. "Computer Software" refers to digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

d. "Client/Server Computing": Computers on the Internet are identified by the type of function they perform. A computer that provides resources for other computers on the Internet is known as a "server." Servers are known by the types of service they provide, that is, how they are configured. For example, a "web server" is a computer that is configured to provide web pages to other computers requesting them. An "e-mail server" is a computer that is configured to send and receive electronic mail from other

computers on the Internet. A "client computer" is a computer on the Internet that is configured to request information from a server. If a client computer is configured to browse web pages and has web page browsing software installed, it is considered a "web client."

e. "Computer system and related peripherals, and computer media" refer to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

f. "Wireless telephone": A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

g. "Internet Service Providers ("ISPs")" and the Storage of ISP Records: Internet Service Providers are commercial organizations that are in business to provide individuals and businesses access to the Internet in exchange for a fee. ISPs provide a range of services for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers (defined below) and other communications equipment. ISPs can offer a range of options in providing access to the Internet, including telephone-based dial-up, broadband-based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data (called bandwidth) supporting the connection to the Internet. Many ISPs assign each subscriber an account name, a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password. ISPs maintain records ("ISP Records") pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). ISP Records may include account application information, subscriber and billing information, account access information

(often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both temporary and long-term storage of electronic communications and many other types of electronic data and files. Typically, e-mail that has not been opened by an ISP customer is stored temporarily by an ISP incident to the transmission of that e-mail to the intended recipient, usually within an area known as the home directory or mailbox. Such temporary, incidental storage is defined by statute as "electronic storage," *see* 18 U.S.C. § 2510(17), and the provider of such a service is an "electronic communications service." An "electronic communications service," as defined by statute, is "any service that provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long-term storage services to the public for electronic data and files, is defined by statute as providing a "remote computing service." 18 U.S.C. § 2711(2).

h. "Internet Protocol Address ("IP Address")" refers to the unique address assigned to every computer or device on the Internet, the same way that every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 69.116.211.141. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ "dynamic" IP addressing, that is, they allocate any unused IP address at the time of initiation of an Internet session to the customer or subscriber gaining access to the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time, and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next dial-up customer. On the other hand, some ISPs, including some cable providers, employ "static" IP addressing, that is, a customer or subscriber's computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer.

i. "Domain Name" refers to the common, easy to remember names associated with an Internet Protocol address (defined below). For example, a domain name of "www.usdoj.gov" refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delineated by a period. Each level, read backwards—from right to left—further identifies parts of an organization. Examples of first level, or top-level domains are typically ".com" for commercial organizations, ".gov" for the United States government, ".org" for

organizations, and ".edu" for educational organizations. Second level names will further identify the organization, for example "usdoj.gov" further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable.

j. "Website" refers to a compilation of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language ("HTML") and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol ("HTTP").

k. "Universal Resource Locator ('URL')" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the web's browser address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies the specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

l. "Website Hosting" provides the equipment and services required to host and maintain files for one or more websites and to provide rapid Internet connections to those websites. Most hosting is "shared," which means that multiple websites of unrelated companies are on the same server in order to reduce associated costs. When a client develops a website, the client needs a server and perhaps a web hosting company to host it. "Dedicated hosting" means that the web hosting company provides all of the equipment and assumes all of the responsibility for technical support and maintenance of a website. "Co-location" means a server is located at a dedicated hosting facility designed with special resources, such as a secure cage, regulated power, climate control, a dedicated Internet connection, online security and online technical support. Co-location facilities offer customers a secure place to physically house their hardware and equipment as opposed to keeping it in their offices or warehouse, where the potential for fire, theft, or vandalism is greater.

m. "Media Access Control Address (MAC Address)" refers to a unique identifier assigned to most devices that access the Internet. Generally, MAC Address information is captured in the networking device, or router, that is the access point to the Internet from most residences or businesses. Reference to this MAC Address information enables identification of the particular device used to access the Internet during a particular session, especially in residences or businesses where more than one device may be used to access the Internet using the same IP Address.

n. "Log File(s)" refer to records that are produced automatically by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.

o. "Cache" refers to text, image, and graphic files sent to and temporarily stored by a user's computer from a website accessed by the user in order to allow the user speedier access to and interaction with that website in the future.

p. "Modem" is an electronic device that allows one computer to communicate with another.

q. "Trace Route" refers to an Internet debugging tool used to document the list of inter-connected computers between two computers on the Internet. A trace route will list the names and IP addresses of computers that provide the physical link between two computers on the Internet. Trace routes are useful tools to help geographically identify where a computer on the Internet is physically located, and usually includes information about the registered owners of computers on the Internet.

r. The terms "records," "documents," "materials," "files," "logs," "ledgers," and the like, include all information created, recorded or stored in any form, visual or aural, by any means, whether in handmade form (including, but not limited to, writings, drawings, paintings), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing), or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs ("CDs"), electronic or magnetic storage devices such as diskettes, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device), and in any location, including locked containers.

III. Child Pornography Collector Characteristics and Use of Computers

A. Collector Characteristics

11. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals who produce, distribute, receive, and/or collect child pornography:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses (such as in person, in photographs, or other visual media), or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, video tapes, computers, DVDs,

books, slides and/or drawings or other visual media. Child pornography collectors often use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child victim, or to demonstrate the desired sexual acts.

c. They often use the Internet to grow their collections. The Internet is used because images and videos containing child pornography abound on the Internet and can be downloaded by consumers of child pornography with relative anonymity. Further, computers and electronic media are generally employed to store images and videos of child pornography because they can hold a tremendous amount of data and allow users to employ passwords and other protections to keep their child pornography collections secure.

d. They sometimes possess and maintain any "hard copies" of child pornographic material that may exist—that is, their printed pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc.—in the privacy and security of their home or some other secure location.

e. These individuals typically retain depictions of child pornography, including images, pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and video tapes for many years.

f. Likewise, they often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a smart phone, a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the collector to view the collection, which is valued highly.

g. They also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

h. They prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.

B. Use of Computers by Collectors of Child Pornography

12. Based upon my knowledge, training, and experience, and the experience and training of other law enforcement officers in child exploitation and child pornography investigations with whom I have had discussions, the development of computers and cellular telephones has revolutionized the way in which those who seek out child pornography are able to obtain this material.

Computers serve several basic functions in connection with child pornography, including production, communication, distribution, and storage. More specifically, the development of digital technology has changed the methods used by those who seek to obtain access to child pornography in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera, and from a smart phone. The camera is attached using a device such as a cable, or digital images are often uploaded from the camera's memory card directly to the computer or through wireless technologies. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs which allow subscribers to dial a local number or otherwise directly connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

c. The ability to produce child pornography easily, reproduce it inexpensively, and distribute it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via cellular telephone, smart phone, e-mail, or through file transfer protocols to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide e-mail service, chat services (*i.e.*, "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

d. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute or receive child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes, the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the

recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient.

e. With Internet access, a computer or cellular telephone user can transport an image file from the Internet or from another user's device to his own device, so that the image file is stored in his device. The process of transporting an image file to one's own computer or cellular telephone is called "downloading." The user can then display the image file on his computer or cellular telephone screen, and can choose to "save" the image on his device and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

f. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single disc can store thousands of images and millions of pages of text, and removed storage devices such as thumb drives have even more capacity. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously over the last several years. Hard drives with the capacity of 500 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

g. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a particular computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or "slack" space—that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

C. <u>Social Media Networks for Sharing Child Pornography</u>

13. The Internet has allowed the collectors and distributors of child pornography to interact on Social Media networks, such as Kik, Snapchat, Facebook, Tumblr, and/or other similar sites that

allow users to interact and engage in both conversations and the exchanging of images and/or videos. There is a legitimate exchange of information and content on these platforms, but they may also have illicit content as well.

14. Your affiant is aware that many child pornography offenders utilize social media sites to locate, meet and/or groom potential minor victims. These sites allow offenders to operate using anonymous identities with access to large numbers of minors and "like minded" individuals.

15. One of the social media sites mentioned above it Tumblr. This site is described as a microblogging and social media website. The site was founded in 2007 and is headquartered in New York City. The site allows users to post blogs or short videos. Analysis conducted by TechCrunch in 2012, showed that 22 percent of Tumblr content was pornography. Individual users can upload videos and the site is self-censored. Your affiant is aware that Tumblr is one of several social media sites where individuals go to both upload and obtain child pornography.

IV. Probable Cause to Search the SUBJECT PREMISES

16. FBI agents have determined that an individual at the **SUBJECT PREMISES** has possessed and/or produced and/or distributed images of child pornography using a computer and/or an electronic device, such as a smart phone or iPad, which is believed to be located at the **SUBJECT PREMISES**. For the reasons set forth below, there is probable cause to believe that evidence of the distribution and/or possession and/or production of child pornography will be located at the **SUBJECT PREMISES**.

17. On March 11, 2020, Minor Male #1 came to one of the FBI's offices to report a subject who had caused him to produce pornographic images of himself when he was a minor living outside of Virginia.

18. Minor Male #1 advised that approximately 6 years ago, when he was fifteen years old, he posted a video to social media showing his fitness transformation. In response to that video, he

was contacted by ELLIOTT ATWELL, who did and currently lives in Albemarle County, Virginia, which is located in the Western District of Virginia.

19. ATWELL told Minor Male #1 that he could help him with his fitness routine, nutrition plan, and physical development. ATWELL began contacting Minor Male #1 by various electronic means, including through social media accounts (such as Snap Chat and Instagram), iMessage, cellphone text messages, and telephone calls.

20. Minor Male #1 described ATWELL as involved in every aspect of his life. ATWELL contacted Minor Male #1 daily and would talk to him about a variety of topics. After a short time into their online interaction, ATWELL began discussing sexual intercourse and sexuality with Minor Male #1.

21. Minor Male #1 advised that ATWELL became increasingly more inquisitive about Minor Male #1's body, finally encouraging him to take images of his erect penis and send them to ATWELL via electronic means. ATWELL also encouraged Minor Male #1 to create videos of himself masturbating to send to ATWELL via electronic means. ATWELL then convinced Minor Male #1 to make pornographic videos of himself engaging in sexual activity with his minor age girlfriend. Minor Male #1 advised he did this and sent them to ATWELL at his direction via electronic means.

22. Leading up to the production, and continuing after he began producing pornographic images, ATWELL also sent gifts to Minor Male #1, to include shoes, knives, alcohol, sex toys, penis enhancement pills, and underwear. These gifts were sent from ATWELL to Minor Male #1's residence outside of Virginia through the United States Postal Service or other package delivery services. Based on my training and experience in child pornography cases, such gifts are often used to groom victims as well as to lower their inhibitions.

23. Minor Male #1 advised that the production of pornography continued into his senior year of high school, when he was 18 years of age. Minor Male #1 recalled either being 17 or 18 years

old when he had an assignment due for school. ATWELL advised Minor Male #1 that he would write the assignment for Minor Male #1 in exchange for a pornographic video of Minor Male #1 having intercourse with his girlfriend. Minor Male #1 advised that ATWELL persisted requesting such videos throughout his entire senior year of high school until Minor Male #1 finally produced the video and sent it to ATWELL.

24. Minor Male #1 advised that he would upload his pornographic videos to his Google One drive for ATWELL to access, so he could download the content. Minor Male #1 describes keeping track on the exact time it would take for the download and being very anxious and upset that ATWELL was violating him, but he describes feeling trapped an obligated to constantly produce these images.

25. Minor Male #1 advised that he was discussing ATWELL with other minor-aged athletes at a recent event. After talking to Minor Male #2, Minor Male #1 became aware that ATWELL was engaging in the same exploitive behavior with several of the other minor male athletes. Specifically, Minor Male #1 became aware that ATWELL was using some of the pornographic images and videos of Minor Male #1 to get the other males to produce images of the minor engaged in sexually explicit activity.

26. Minor Male #1 also became aware that ATWELL was sending or had sent several of the other minor males sex toys, sexual enhancement pills, clothing, and other items to facilitate and encourage the production of the child pornography. In addition, Minor Male #1 was aware that ATWELL had purchased several hotel rooms for the minor males at a recent fitness event, including an extra room he wanted the minor males to film themselves having sex with girls and send it to him. ATWELL did not attend the event, but did pay for several of the minor males to attend.

27. Minor Male #1 advised that it was at that point that he realized he had to disclose ATWELL's behavior and could not allow ATWELL to keep exploiting minor males. Minor Male #1

advised he told the other athletes that ATWELL had exploited him and they needed to stay away from him and stop sending ATWELL images. Minor Male #1 advised some of the males became very emotional. Minor Male #1 advised that his disclosure was repeated by several males at the event, and it exploded on social media.

28. Your affiant interviewed Minor Male #2, who is currently 17 years of age. Minor Male #2 advised he met ATWELL via the Internet. ATWELL commented on his social media post and offered to give him advice on nutrition and fitness. Minor Male #2 advised that ATWELL has tried to get him to send images of his penis to him, but he has only sent images of his buttocks.

29. Minor Male #2 advised that ATWELL has sent him various gift via the mail to include:

a. Sex Toys

b. Penis Pump

c. Clothing to include underwear.

d. Knives

e. Penis enhancement medications.

30. The mother of Minor Male #2 advised that she intercepted a package sent to Minor Male #2. This package was turned over to the FBI, and the following was noted:

a. The package was addressed to Minor Male #2's home address outside of Virginia.

b. The package address also included the name "United States," indicating it likely came from outside of the United States.

c. The package was shipped by EMS Speed Post, with the number 434-249-6298 written on the package and the barcode: ED903665123IN. This is the cellphone number belonging to ATWELL.

d. The package contained 4 blue pills with the label Nizagara 100 mg tablet (Sildenafil Citrate Tablet). The package also contained 20 pills of Sildenafil and Dapoxetine tablets. Your affiants is aware that these drugs are commonly used to enhance erections in men.

31. The barcode for EMS Speed Post indicates originated in India. Minor Male #2 was fifteen years old when this package was received at his residence in the United States.

32. Minor Male #2 also advised ATWELL had sent him many other personal items and he was afraid his parents would find out about them.

33. Minor Male #2 advised that he recently disclosed to Minor Male #1 what was going on with ATWELL and that Minor Male #1 told him that ATWELL had exploited him for years.

34. Minor Male #2 advised that after ATWELL's actions became public, ATWELL called him on his cellphone and left a message apologizing for his behavior and saying he should not have violated peoples' trust the way he did. ATWELL cried on the message saying he hoped to make it up to Minor Male #2 so they could still be friends.

35. Minor Male #2 communicated with ATWELL on his cell phone number 434-249-6298, through calls, texts, and/or iMessage. Minor Male #2 also communicated with ATWELL via his social media accounts. Minor Male #2 was aware that ATWELL was active on Facebook.

36. The FBI had contact with another male identified as Minor Male #3. Minor Male #3 advised that he had met ATWELL via social media. ATWELL had befriended him because Minor Male #3 was friends with Minor Male #1.

37. Minor Male #3 advised that ATWELL became a confidante, someone he spoke to everyday. Very shortly after starting his relationship with ATWELL, the conversations turned to sexual topics. ATWELL wanted Minor Male #3 to send penis pictures, which he did. In addition, Minor Male # 3 was also asked to produce a pornographic video of him having sexual intercourse with

a female at the direction of ATWELL. Minor Male #3 was living outside of Virginia during the time period he was producing pornographic images for ATWELL and provided the images and videos to ATWELL via electronic means.

38. Minor Male #3 advised that he believes he was 17 years old when he produced the first image he sent to ATWELL. Minor Male #3 is unsure of his age when he sent ATWELL videos of him having sexual intercourse with a female, but is positive the female was only 17 years old at the time of the production of the video.

39. Minor Male #3 advised that beginning when he was a minor ATWELL would send him gifts to include:

a. Sex Toys

b. Penis Pump

c. Clothing to include underwear.

d. Knives

e. Penis enhancement medications.

40. Minor Male #1 advised that when he was a minor, his uncle drove him to ATWELL's home in Virginia. Minor Male #1 provided the following information on ATWELL's residence:

a. The address is 1133 Oak Hill Drive, Charlottesville, Virginia, which is the **SUBJECT PREMISES**.

b. ATWELL lives at home with his mother and father. They are the only residents.

c. ATWELL's residence is a single family, single story detached residence in a suburban neighborhood.

d. Minor male #1 advised ATWELL is obsessed with guns and knives and lots of them are in his residence.

41. Minor Male #1 identified an unlabeled photograph as ATWELL. Your affiant is aware that the image was from the Commonwealth of Virginia's Department of Motor Vehicle (DMV) records. Virginia DMV lists ATWELL's home address as 1133 Oak Hill Drive, Charlottesville, Virginia.

42. Your affiant has obtained subscriber records for cellular telephone number 434-249-6298 from AT&T. These records indicate the following:

a. Subscriber: ELLIOTT ATWELL

b. Address: 1133 Oak Hill Drive, Charlottesville, VA 22902

c. Contact Email: ABRELLIOTT@GMAIL.COM

d. Service Start Date: 03/08/2009 and still active.

e. Additional Contact: MR1911@VT.EDU.

43. Your affiant has reviewed call detail records associated with 434-249-6298. These records appear to indicate that prior to March 12, 2020, ATWELL was using an iPhone X Max. After March 12, 2020 ATWELL appears to be using an iPhone 11 Max. Your affiant is aware that most users back up their iPhones up from one model to the next so they do not loose content. In addition, users may keep some content on their phone and other content in a remote location or external device to protect the content.

44. In March 2020, a CLEAR database check revealed that ATWELL is listed as residing at the **SUBJECT PREMISES** from September 2008 – January 2019 (Experian) and from January 1989 – November 2018 with a possible telephone number of (434) 249-6298.

45. On March 13, 2020, a physical surveillance was completed of the **SUBJECT PREMISES**. A grey 4 door Nissan sedan bearing Virginia registration VML-3296 was observed parked in the gravel driveway of the **SUBJECT PREMISES**. A check of the Virginia Department of Motor Vehicles records indicates the Nissan sedan bearing Virginia registration VML-3296 is a

2012 Nissan registered to ALAN WAYNE ATWELL of 1133 Oak Hill Drive, Charlottesville, Virginia 22902.

46. On March 19, 2020 a surveillance was completed of the **SUBJECT PREMISES**. Three vehicles were observed parked in the driveway of the **SUBJECT PREMISES**. A brief video was taken, but due to low light conditions, no license plate numbers or lettering were visible. The vehicles included a 4-door Nissan Sedan, a 4-door Chrysler 300, and a 4-door Chevrolet Suburban/Tahoe.

47. On April 16, 2020, April 30, 2020, and May 7, 2020 surveillance was completed of the **SUBJECT PREMISES**. Three vehicles were observed parked in the driveway of the **SUBJECT PREMISES**. Brief videos were taken. The vehicles included a 4-door Nissan Sedan, a 4-door Chrysler 300, and a 4-door Chevrolet Suburban/Tahoe.

48. W-1 has informed the FBI that ATWELL drives a Chrysler 300 with Virginia tags VVZ-6888. (W-1 knows ATWELL and has had interactions with him in the past.) The Virginia DMV database shows that a Chrysler 300 with Virginia license plate VVZ-6888 is registered to ATWELL at the **SUBJECT PREMISES**. Based on the surveillance, information from W-1, and information from the Virginia DMV database, it appears that ATWELL still resides at the **SUBJECT PREMISES**.

49. Collectors of child pornography will hide their collections from others, including from parents and spouses. Because of the small size and portability of electronic devices, such as iPhones, iPads, and laptops, as well as the small size of media storage devices, ATWELL's vehicle may be a storage location for items referenced in Attachment B that contains evidence of the Specified Federal Offenses.

50. Based upon my knowledge, training, and experience, and the experience and training of other law enforcement officers in child exploitation and child pornography investigations with

whom I have had discussions, I am familiar with the practices and methods of persons who produce, distribute, receive, and/or collect child pornography, and their reliance on computer technology to commit these criminal offenses. Such individuals often create and maintain records relating to these offenses, including, but not limited to, images, videos, correspondence, documents, and the names of victims and other individuals engaged in these offenses, on electronic databases on the computers, stored in electronic or magnetic form. Furthermore, users of computer equipment often create and maintain records of computer ownership and subscriptions to internet services. Based on this information, and on the facts set forth above, there is probable cause to believe that there is evidence, contraband, fruits, instrumentalities of child pornography and computer-related equipment that may contain evidence of the Specified Federal Offenses located at the **SUBJECT PREMISES**.

V. Search and Seizure

51. As used in this affidavit, the term "electronic storage media" includes all equipment that can store, collect, analyze, create, display, convert, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, self-contained "laptop" or "notebook" computers, and cellular telephones and "smartphones, and tablets such as iPads); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, and other memory storage devices, such as thumb drives); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); related communication devices (such as routers, modems, cables, and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

52. As described above and in Attachment B, this application seeks permission to search for evidence of the Specified Federal Offenses that might be found on electronic media located at the **SUBJECT PREMISES**, in whatever form they are found. One form in which evidence might be found is data stored on electronic storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

53. I submit that if electronic storage media is found on the **SUBJECT PREMISES**, there is probable cause to believe evidence of the Specified Federal Offenses will be stored on that electronic storage media, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space — that is, in space on the storage medium that is not currently being used by an active file — for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, electronic storage media — in particular, computers' internal hard drives — contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

54. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but

also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the **SUBJECT PREMISES** because:

a. Data on the electronic storage media can provide evidence of a file that was once on the storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage media that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage media that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on electronic storage media can also indicate who has used or controlled the media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the electronic storage media at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on electronic storage media that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a particular electronic storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

55. I know that when an individual engages in the Specified Federal Offenses the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

56. In most cases, a thorough search of a premise for information that might be stored on electronic storage media requires the seizure of the physical media and later off-site review consistent with the warrant. In lieu of removing electronic storage media from the premises, it is sometimes possible to make an image copy of the media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the electronic storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. Searching computer systems is a highly technical process, which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to list them all. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing 500 gigabytes (GB) of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 250 million pages of data, which, if printed out, would result in a stack of paper over ten miles high. Further, a 500 GB drive could contain as many as approximately 250 full run movies or 450,000 songs.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography, a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or instrumentalities of a crime.

57. Based on the foregoing, and consistent with Rule 41(e)(2)(B), when persons executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit seizing or imaging electronic storage media that reasonably appear to contain some or all of the evidence described in the warrant, thus permitting its later examination consistent with the warrant. The examination may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

58. In anticipation of litigation relating to the authenticity of data seized pursuant to the Warrant, the Government requests that it be allowed to retain a digital copy of all seized information authorized by the Warrant for as long as is necessary for authentication purposes.

59. Based on my own experience and my consultation with other agents who have been involved in computer searches, searching computerized information for evidence or instrumentalities of a crime often requires the seizure of all of a computer system's input and output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. There are several reasons that compel this conclusion:

a. The peripheral devices that allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence listed above. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices; and

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices, as well as the central processing unit ("CPU"). In cases such as this, where the evidence consists partly of graphic image files, the monitor and printer are also essential to show the nature and quality of the graphic images that the system can produce. Moreover, the keyboard, modem and other system components were used as a means of committing the child pornography offenses at issue, including accessing the Internet, communicating with other computers, and storing child pornography. The analyst also needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media), as well as all related instructional manuals or other documentation and security devices, for proper data retrieval.

c. It would be impossible to access the system if it is password protected or if other encryption devices are in place. Users often record passwords or keys on material found near the computer system. These passwords or keys could be names or a combination of characters or symbols.

60. In light of these concerns, I hereby request the Court's permission to search the **SUBJECT PREMISES** and to copy, image, and seize the computer devices (and associated peripherals) that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search for the evidence described in Attachment B.

61. I am familiar with and understand the implications of the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, and the role of this statute in protecting First Amendment activities. I am not aware that any of the materials to be searched and seized from the **SUBJECT PREMISES** are protected materials pursuant to the PPA. If any such protected materials are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

SEALING ORDER REQUESTED

62. It is respectfully requested that this Court issue an order sealing, until further order of this Court, all papers submitted in support of this application, including the application, affidavit, and search warrant, and the requisite inventory notice (with the exception of one copy of the warrant and the inventory notice that will be left at the **SUBJECT PREMISES**). Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation, and premature disclosure of the contents of this Affidavit and related documents may jeopardize the effectiveness of the investigation.

BIOMETRIC ORDER REQUESTED

63. In my training and experience, it is likely that the **SUBJECT PREMISES** will contain at least one Apple brand device, such as an iPhone or iPad, because AT&T records appear to indicate that prior to March 12, 2020, ATWELL was using an iPhone X Max. After March 12, 2020 ATWELL appears to be using an iPhone 11 Max. The **SUBJECT PREMISES** may also contain other cellphones.

64. I know from my training and experience, as well as from information found in publicly available materials including those published by cellphone manufacturers, such as Apple, that some models of electronic devices, such as iPhones and iPads, offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") or form of facial recognition software in lieu of or in combination with a numeric or alphanumeric passcode or password.

65. If a user enables this fingerprint or facial recognition coding on a given electronic device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. Facial recognition software works by allowing the user to hold the electronic device at a certain angle to their face to unlock the device. In my training and experience, users of devices that offer these tools often enable them because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

66. In some circumstances, a fingerprint or face cannot be used to unlock a device, and a passcode or password must be used instead. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked device, the opportunity to unlock the device via Touch ID or facial recognition software exists only for a short time. Touch ID also will not work under other circumstances.

67. The passcode or password that would unlock the electronic devices found during the search of the **SUBJECT PREMISES** is not known to law enforcement. Thus, it will likely be necessary to press the finger(s) of the user(s) or use the user's face in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. Attempting to unlock the relevant device(s) via Touch ID or with facial recognition software with the use of the fingerprints or facial image of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

68. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user who can unlock the device, and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it will likely be necessary for law enforcement to have the ability to require any occupant of the **SUBJECT PREMISES** to press their finger(s) against the Touch ID sensor of the locked device(s) or hold the device up to their face found during the search of the **SUBJECT PREMISES** in order to attempt to identify the device's user(s) and unlock the device(s) via Touch ID or facial recognition software.

69. Although I do not know which of a given user's 10 fingerprints is capable of unlocking a particular device, based on my training and experience I know that it is common for a user to unlock a Touch ID-enabled Apple device via the fingerprints on thumbs or index fingers. In the event that law enforcement is unable to unlock the device(s) found in the **SUBJECT PREMISES** as described

above within the five attempts permitted by Touch ID or facial recognition software, this will simply result in the device requiring the entry of a password or passcode before it can be unlocked.

70. Due to the foregoing, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the **SUBJECT PREMISES** to the Touch ID sensor of the device(s), such as an iPhone or iPad, found at the **SUBJECT PREMISES** for the purpose of attempting to unlock the device via Touch ID in order to search the contents as authorized by this warrant. Similarly, I request that the Court authorize law enforcement to hold up the device(s) to faces of individuals found at the **SUBJECT PREMISES** to use any facial recognitions software.

71. We believe ATWELL to be dangerous. ATWELL weighs nearly 300 pounds and is known as a powerlifter that is armed with a handgun and has a concealed carry permit. ATWELL is reportedly a gun fanatic and is obsessed with handguns, rifles, and knifes. For example, ATWELL has an email account "Mr. 1911," referring to a 1911 handgun. Many of his online conversations with victims revolve around weapons. ATWELL is also known to carry firearms on his person. A local gym owner stated that he had to tell ATWELL numerous times not to continue to bring his firearm into the gym and to leave the firearm in his vehicle. ATWELL has also posted on social media a video of him and friends shooting handguns and rifles outdoors. In text conversations, ATWELL discusses ordering “scopes” and getting a custom barrel for his Glock.

72. In addition, on social media, ATWELL expresses views against law enforcement. In open social media accounts, ATWELL expresses the need of citizens to violently oppose any infringement on individual liberties by law enforcement and advocates the use of violence. Additionally, in several text communications (somewhat dated or older texts), ATWELL discusses suicidal ideation. This ideation is centered around him being outed as "gay" or homosexual, and his inability to control his sexual desires towards adolescent males (images).

73. I believe that ATWELL is a danger to law enforcement, his own family, and himself. In light of these concerns, I hereby request the Court's permission to execute the search warrant on the **SUBJECT PREMISES** at anytime. This will allow for greater law enforcement safety by utilizing the cover of darkness.

CONCLUSION

74. Based on the above information, there is probable cause to believe that the Specified Federal Offenses, which, among other things, make it a federal crime for any person to knowingly possess, receive, and distribute child pornography, have been violated and that evidence, contraband, fruits, and instrumentalities of a crime, as described in Attachment B, are located at the **SUBJECT PREMISES**.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Philipp W. Alhusen
Philipp W. Alhusen, Special Agent
Federal Bureau of Investigation

Received by reliable electronic means and sworn and attested to by telephone on this 12th day of May 2020.

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE